Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	**GN Docket No. 13-111**
	)	
	)	

COMMENTS OF SCREENED IMAGES, INC. D.B.A. CORRECTIONS.COM

Dated: July 17, 2017

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	**GN Docket No. 13-111**
	)	
	)	
	)	

COMMENTS OF SCREENED IMAGES, INC. D.B.A. CORRECTIONS.COM

INTRODUCTION

Screened Images, d.b.a Corrections.com (Corrections.com), a Massachusetts Woman-Owned small business, has been a leader in the Corrections industry for over twenty years. With twenty Managed Access Systems (MAS) deployed in the United States, Corrections.com has more practical and technical experience than any other MAS provider. Corrections.com appreciates the Commission's support and attention to the matter of combating contraband devices in correctional facilities and is grateful for the opportunity to provide comment on this important public safety issue.

I. THE COMMISSION SHOULD ALLOW FOR THE TERMINATION OF CONTRABAND WIRELESS DEVICES

It is imperative that the Commission takes action to permanently prevent contraband wireless devices from operating on the network of any CMRS provider. Permanent termination of service to these devices will provide a safer work

environment for correctional facility staff, protect members of the public, and end the black market for wireless devices inside correctional facilities.

In its comments, Verizon makes the statement that "(d)eploying effective MAS technologies should make cell detection and service termination systems unnecessary."[1] While Corrections.com understands Verizon's position, the operational realities of correctional facilities (e.g. physical location, site layout, presence of visitors, inmate work programs, the existence of a black market for contraband commodities), create a unique environment in which permanent service termination would further the ultimate goal of eliminating contraband wireless devices from correctional facilities.

Managed access technology is extremely effective within the predetermined coverage areas. Prior to deployment, these coverage areas are determined based on the needs of the respective public safety agency and the physical layout of the facility. As a result, there are opportunities for some inmates to utilize contraband wireless devices outside of the MAS coverage area. For example, most correctional facilities have inmate work programs that allow inmates to perform jobs outside the secured perimeter of the facility or in some cases, off property. While outside of MAS coverage, these inmates are able to use contraband wireless devices to make voice calls, send text messages, take and distribute photos and videos, utilize social media, and carry on criminal enterprises. In addition, inmates involved in work programs outside the MAS coverage area may use these contraband wireless

[1] GN Docket 13-111, Comments of Verizon at 3 (June 19, 2017).

devices to carry out the agendas of higher security inmates. Permanently terminating service to these devices will prevent inmates from taking advantage of time outside the MAS coverage area and will further the goals of providing a safer work environment for correctional facility staff and protecting members of the public.

Another reality of correctional facilities is the existence of black markets for contraband commodities, including wireless devices. The high price inmates are willing to pay for contraband wireless devices has created a lucrative business opportunity for individuals both inside and outside of correctional facilities. Permanently denying service will render these devices useless, eliminating the demand and thus, the incentive to smuggle devices into facilities. By eliminating the return on investment from the purchase of contraband wireless devices, the Commission has the opportunity to effectively end this black market.

II. THE COMMISSION SHOULD ADOPT A COURT-ORDERED APPROACH FOR THE TERMINATION OF CONTRABAND WIRELESS DEVICES

Corrections.com concurs with CTIA and the CMRS providers that requiring judicial review and a court order is the optimal process for terminating service to contraband wireless devices.[2] Obtaining a court order will ensure that service is only terminated when there is substantial evidence that the device is in fact, contraband. Corrections.com concurs with T-Mobile's argument that a court order "would be consistent with the checks and balances traditionally imposed by the

[2] GN Docket 13-111, Comments of CTIA at 5-6 (June 19, 2017); Comments of Verizon at 6 (June 19, 2017); Comments of T-Mobile at 4-5 (June 20, 2017); Comments of AT&T at 9 (June 19, 2017).

government when illegal activity is suspected."[3] Further, Corrections.com concurs with Verizon's statement that "a licensee should not be responsible for verifying or investigating the accuracy of a service termination request, as suggested in the *Further Notice*."[4] Requiring a court order ensures that the CMRS providers are not burdened with tasks best left to public safety agencies, managed access providers, and the courts.

Corrections.com knows firsthand that without FCC action it will not be possible to obtain a court order for the termination of service to contraband devices. In a previous attempt to obtain such a court order, Corrections.com worked closely with a state department of corrections and the District Attorney for the respective jurisdiction. However, the District Attorney has stated that without a law explicitly allowing for the termination of service to contraband devices located in correctional facilities, and no legal precedence to cite, the court is unwilling to issue a warrant. Enacting such a federal law would provide the authority necessary for the courts to issue these warrants.

Under a court-ordered approach, the issuance of a warrant would allow public safety agencies to request important forensic data from both the CMRS providers as well as the inmate phone service provider. As AT&T stated in their comments, "(b)y requiring a court order, the Commission will create a framework in which wireless carriers can share relevant evidence with law enforcement without

[3] GN Docket 13-111, Comments of T-Mobile USA, Inc. at 5 (June 20, 2017).
[4] GN Docket 13-111, Comments of Verizon at 7 (June 19, 2017).

violating rules governing customer privacy."[5] This data may be useful to public safety agencies and law enforcement as part of ongoing criminal investigations, which may contribute to enhanced safety for both correctional staff and the public.

Should the Commission decide to forego a court-ordered approach in favor of a rule-based approach to service termination requests, it should require strong evidence that the device is a verifiable contraband wireless device. Other CIS providers also support the idea that substantial evidence should be in place prior to the termination of service.[6] No single piece of data is enough to make the determination as to whether a phone is contraband or not. As such, Corrections.com recommends that the Commission require the requesting party demonstrate a facility-based historical trend of contraband usage, using multiple pieces of data. Specifically, the Commission should require that evidence include data such as:

- Historical timeframes during which phone is used;
- Destination numbers (e.g. evidence that device is dialing numbers on the facility's staff recall list vs. numbers on the inmate phone provider's known inmate call list);
- Usage and destination numbers dialed over a period of time;
- Contents of attempted SMS messages;
- Unique identifiers (e.g. MEID, IMEI, IMSI);
- If available, evidence that device has or has not moved between facilities.

[5] GN Docket 13-111, Comments of AT&T at 11 (June 19, 2017).
[6] GN Docket 13-111, Cellblox Notice of Ex Parte (March 15, 2017).

The aggregation of this data, when analyzed by the managed access system, will create a compelling case as to whether a device is contraband and should be subject to service termination. For example, a device that continuously registers on the MAS, dials numbers on the inmate telephone provider's approved inmate call list, and sends SMS messages that include an inmate identification number, address or other information suggesting phone is being used as a contraband device, presents a strong case that the device should be subject to service termination. Alternatively, a device that registers on the MAS during times that align with staff work schedules, dials numbers on the facility's staff recall list, and sends SMS messages that suggest the person leaves the facility regularly, presents a strong case that the device should not be subject to service termination.

Some CIS providers advertise their ability to capture unique identifiers from all wireless devices on property. However, the unique identifier alone does not provide public safety agencies, the courts, or the CMRS providers with conclusive evidence that device is contraband and should be subject to service termination.[7] Managed access systems gather multiple sources of evidence and perform the historical analysis necessary to show facility-based patterns of contraband usage, ensuring CMRS providers that service terminations are justified.

Whether a device is identified as contraband through a court-ordered or rule-based approach, Corrections.com recommends that the device be entered into a database similar to the stolen smart phone database. Once entered into the

[7] GN Docket 13-111, "Response to FCC Request for Interfering with Cell Phone Communication", CellAntenna at 1 (July 18, 2013).

database, the current CMRS provider would be required to terminate service and all other CMRS providers would be prohibited from providing future service to the device. Verizon points out that "cover(ing) all service providers serving the correctional facility's area – not just the user's current network…minimize(s) inmates' ability to circumvent a request by swapping out SIM cards."[8] The California Department of Corrections and Rehabilitation has also supported the permanent termination of service to devices identified as contraband.[9] Corrections.com concurs with Verizon and CDCR in supporting the permanent termination of service to contraband devices. Further, Corrections.com believes that a contraband phone database aligns with the Commission's goal of facilitating a "nationwide solution."[10]

III. THE COMMISSION SHOULD NOT REQUIRE CMRS PROVIDERS TO PROVIDE NOTIFICATION TO CIS PROVIDERS PRIOR TO MAKING NETWORK CHANGES

Corrections.com does not support the proposal that CMRS providers should be required to provide notification to CIS providers prior to making network changes. While Corrections.com does believe that cooperation from the CMRS providers is important to the success of any CIS, notification of network changes is unnecessary. As part of its maintenance program, Corrections.com conducts regularly scheduled analysis of signals present at MAS deployment locations. Further, all future deployments and upgrades to existing managed access systems will include automated remote spectrum scanning capabilities.

---

[8] GN Docket 13-111, Comments of Verizon at 9 (June 20, 2017).
[9] GN Docket 13-111, Comments of CDCR at 4 (July 18, 2013).
[10] *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Report and Order and Further Notice of Proposed Rulemaking, FCC 17-25 at 32 (2017).

In Corrections.com's experience, the CMRS providers do provide advance notification of major network changes. For example, during the recent AT&T and T-Mobile spectrum swaps, which impacted several MAS deployments, Corrections.com worked closely with the CMRS providers. This cooperation from AT&T and T-Mobile made the spectrum swaps seamless for the impacted systems. Since the CMRS providers are voluntarily providing notification of many of their major network changes, Corrections.com does not believe mandated notification requirements are necessary.

Corrections.com recognizes that the frequency with which CMRS providers make network changes, to balance the needs of their customers, it would be over burdensome and near impossible for them to provide notification of each of these changes. While Corrections.com appreciates notification of major network changes, CMRS providers should not be held responsible for performing a function, where technology exists to allow CIS providers to perform this function on their own. Corrections.com concurs with T-Mobile's position that the burden placed on the CMRS providers would outweigh the benefit to CIS providers.[11]

IV. OTHER TECHNOLOGICAL SOLUTIONS

Corrections.com does not support the idea of mandating "quiet zones," which are described in the *Further Notice* as "the creation of areas in which communications are not authorized such that contraband wireless devices in

[11] GN Docket 13-111, Notice of Ex Parte (March 20, 2017).

correctional facilities would not receive service from a wireless provider."[12] Based on experience deploying and maintaining systems that operate on RF spectrum, Corrections.com agrees with the CMRS providers that it would be difficult to design networks that provide optimal service to the public but must "stop at a barbed wire fence."[13] As CTIA has pointed out, this solution may result in denying service to members of the public who live near correctional facilities in rural areas, as service in rural areas often includes "higher power antennas on tall towers that cover great distances."[14] CTIA's concern extends beyond facilities located in rural areas. "Even in urban areas, quiet zones would have to extend substantially beyond the bounds of the prison property."[15] Interfering with the public's ability to access CMRS networks is too great a burden for the public to bear and introduces public safety concerns for those living near or traveling in the vicinity of correctional facilities. For these reasons, Corrections.com concurs with CTIA and the CMRS providers and does not support the implementation of "quiet zones."

The concerns expressed above regarding "quiet zones" also apply to "geolocation-based denial." For those reasons, Corrections.com does not support "geolocation-based denial."

---

[12] *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Report and Order and Further Notice of Proposed Rulemaking, 32 FCC Rcd 2336, at 47 (2017).
[13] GN Docket 13-111, Comments of CTIA at 10 (June 19, 2017).
[14] *Id*. at 10.
[15] *Id.* at 11.

Corrections.com joins the CMRS providers and CTIA in opposing network-based solutions.[16] Corrections.com does not believe that the CMRS provider should be solely responsible for combatting the issue of contraband phones in correctional facilities. As T-Mobile points out in their recent comments, requiring the carriers to track the location of all subscriber devices and deny service to those located at correctional facilities "is technically infeasible because CMRS carriers do not actively track the precise geolocation of their subscribers."[17] Further, imposing this requirement on the CMRS providers raises concerns about customer privacy as it "may be a violation of Section 22 of the Communication Act, which protects certain location information as proprietary customer information."[18]

Even if the CMRS providers had the ability to track the location of all subscriber devices and flag those located at a correctional facility and if privacy were not a concern, Corrections.com does not believe that the CMRS providers are in the best position to determine which devices are contraband. The location of a device does not provide conclusive evidence that a device is contraband. A device located at a correctional facility is not necessarily contraband. Similarly, a device that leaves the correctional facility property may be contraband. Throughout the day many people such as staff, contractors, volunteers, visitors, and even inmates enter and exit correctional facility property. Managed access systems have the continuous data collection capability and forensic tools necessary to determine

[16] GN Docket 13-111, Comments of CTIA at 11 (June 19, 2017); GN Docket 13-111, Comments of Verizon at 12 (June 20, 2017); GN Docket 13-111, Comments of T-Mobile at 17 (June 20, 2017).
[17] GN Docket 13-111, Comments of T-Mobile at 17 (June 20, 2017).
[18] *Id*. at 17.

whether a device has demonstrated a facility-based historical trend of contraband usage.

Corrections.com concurs with the CMRS providers and CTIA in opposing beacon technology as a viable solution to this urgent public safety issue.[19] This solution requires that all wireless devices be manufactured with the software necessary to operate beacon technology. As noted by CTIA and T-Mobile, this would violate the Commission's policy of remaining technology-neutral.[20] Mandating that one type of solution be used over another would negatively impact small businesses that have invested resources into developing solutions. Remaining technology neutral allows for diversity of solutions. Another concern is that this technology is not immediately ready to implement.[21] The problem of contraband devices inside correctional facilities is so pervasive and the public safety concerns are so urgent that the Commission should not mandate a solution that would take years to develop and implement. Rather, the Commission should focus on solutions that are readily available, such as managed access. Finally, and perhaps most importantly, mandating a solution that requires a change to user hardware will almost certainly create the existence of a new black market inside America's correctional facilities, for devices manufactured without the necessary software.[22]

---

[19] GN Docket 13-111, Comments of CTIA at 9(June 19, 2017); GN Docket 13-111, Comments of T-Mobile at 18-19 (June 20, 2017); GN Docket 13-111, Comments of Verizon at 12 (June 20, 2017).
[20] GN Docket 13-111, Comments of CTIA at 10 (June 20, 2017); GN Docket 13-111, Comments of T-Mobile at 18 (June 20, 2017).
[21] GN Docket 13-111, Comments of Verizon at 12 (June 20, 2017).
[22] GN Docket 13-111, Comments of T-Mobile at 19 (June 20, 2017).

CONCLUSIONS

For the above stated reasons, Corrections.com urges the Commission to adopt a court-ordered approach for termination of service to contraband devices. Corrections.com further requests that the Commission not require CMRS providers to provide notification to CIS providers prior to making network changes, and take a technology neutral stance regarding the availability of solutions to combat contraband devices in correctional facilities.

Respectfully submitted,

/s/ Joseph S. Noonan

Joseph S. Noonan
CEO
Screened Images, Inc. d.b.a. Corrections.com

Dated: July 17, 2017